KING & SPALDING

King & Spalding LLP
633 West Fifth Street
Suite 1600
Los Angeles, CA 90071
Tel: +1 213 443 4355
Fax: +1 213 443 4310
www.kslaw.com

CONFIDENTIAL ATTORNEY-CLIENT, COMMON INTEREST PRIVILEGED MEMORANDUM

TO: NSO Group Technologies Limited

FROM: King & Spalding LLP

DATE: November 5, 2020

RE: NSO's Duty to Preserve Electronically Stored Information

I. Executive Summary

This Memorandum addresses the following issues.

(1) **NSO's obligations to the U.S. District Court to preserve electronically stored information ("ESI") remain in effect during the current stay of discovery pending appeal**. Under U.S. law, NSO has an ongoing duty to preserve ESI regardless of the stay of discovery pending appeal. This "duty to preserve" includes all materials likely to be relevant to any party's claim or defense, defined broadly, unless preservation would not be proportional to the needs of the case. (In cases such as the *WhatsApp* litigation, "proportionality" is unlikely to be much of a limitation on preservation or discovery obligations.)

(2) **NSO should follow the "custodian-based" approach typically used to satisfy U.S. court preservation obligations**. To avoid sanctions, the standard practice in significant U.S. litigation is for companies to take a custodian-based approach to preservation, rather than attempting simply to preserve all ESI. In a custodian-based approach, NSO would direct litigation counsel to conduct custodian interviews to assess where information relevant to the lawsuit is stored and to determine the best means of preserving that information. Such an approach would allow NSO to establish it has taken reasonable steps necessary under U.S. law to avoid spoliation sanctions.[1] It would also minimize interruptions to NSO's ongoing business operations, including by avoiding the costs and other burdens associated with "over-preserving" irrelevant information. The only alternative approach under U.S. law to minimize the risk of sanctions is to preserve *all* electronically stored information.

(3) **The Seizure Order does not excuse NSO from U.S. Court preservation obligations and should be modified or clarified**. We understand that the Seizure Order currently in effect

[1] "Spoliation is the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." *Compass Bank v. Morris Cerullo World Evangelism*, 104 F. Supp. 3d 1040, 1051-52 (S.D. Cal. 2015) (citation omitted).

may have been interpreted by the Israeli Department of Justice to prohibit duplication of NSO's ESI, which would be necessary to preservation. NSO should request that the Seizure Order be amended to allow NSO to pursue a custodian-based approach to preserving its ESI and to turn over any preserved ESI immediately to the Government of Israel. If this duplication and turn-over will not be permitted, NSO should request that the Seizure Order be clarified expressly to prohibit NSO from duplicating ESI in any circumstances, so that NSO's inability lawfully to comply with U.S. discovery obligations is clear.

In summary:

(1) Under U.S. law NSO must preserve relevant ESI, either through a custodian-based approach, or a blanket approach for all ESI.

(2) We recommend that NSO undertake a custodian-based approach to preserving ESI to minimize legal risk, expense, and business interruption. Otherwise, NSO must preserve all ESI.

(3) The Israeli Seizure order does not excuse NSO from U.S. preservation obligations. We recommend that NSO request the Seizure Order be amended to allow custodian-based ESI preservation with the Government of Israeli taking immediate possession of any preserved ESI. If this is not possible, the Magistrate Court order should be amended to explicitly make clear that NSO is prohibited from preserving ESI.

II. ESI Preservation Obligations Under U.S. Law

U.S. law authorizes broad discovery. Under U.S. law, any party may "obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case," including relevant hard copy documents and ESI.[2] Courts interpret the terms "document" and ESI very broadly to include almost any type of information that is stored in any medium—potentially including *everything* in the set of data/assets NSO has identified as potentially relevant.[3] A claim that preservation is not proportional would be difficult to establish in a significant case like this one.

If WhatsApp prevails in NSO's appeal and the stay is lifted, NSO may be required to provide information responsive to Plaintiffs' outstanding requests to NSO for production of documents, as well as additional requests Plaintiffs may serve in the future. The stay of discovery does not terminate NSO's preservation obligations with respect to this information. U.S. law requires any party to a litigation to "preserve all relevant documents [and ESI] related to the litigation" in case its future production is required,[4] and a party's duty to preserve discoverable information remains intact during a stay.[5] As we have discussed on several occasions, NSO may

[2] Fed. R. Civ. P. 26(b)(1); *see Zubulake v. Warburg*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003).
[3] Fed. R. Civ. P. 34(a)(1)(A); *see Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443, 447 (C.D. Cal. 2007).
[4] *Apple Inc. v. Samsung Elecs. Co.*, 888 F. Supp. 2d 976, 991–92 (N.D. Cal. 2012).
[5] *See, e.g.*, *Al Otro Lado, Inc. v. Nielsen*, 328 F.R.D. 408, 424 (S.D. Cal. 2018); *Mendoza v. Allied Interstate LLC*, 2017 WL 8161088, at *3 (C.D. Cal. Aug. 7, 2017); *Barr v. Harvard Drug Grp., LLC*, 2015 WL 11181968, at *4 (S.D.

face sanctions, up to and including an order entering judgment against it, if it fails to comply with this duty.[6]

III. Steps to Efficiently Comply with U.S. ESI Preservation Obligations

1. *U.S. Courts Generally Expect a Custodian-Based Approach to Preserve ESI*

NSO's duty to preserve ESI (and other evidence) extends to all information likely relevant to the litigation, including but not limited to the detailed examples listed in the attached Appendix. NSO's duty to preserve information also extends to all the technology and software included in the list of assets that NSO provided on October 26, 2020, because each item on the list would fall within the definition of "electronically stored information." If NSO fails to comply with its duty to preserve ESI, it may face sanctions if relevant information ordered to be produced has been lost and is unavailable. This duty can be violated even inadvertently, for example, if information is lost as a result of employees leaving without preserving relevant ESI, automatic deletion protocols that are not suspended, or technological updates in NSO's business operations that overwrite, delete, or replace ESI.

To accomplish preservation and establish the reasonable steps necessary to avoid sanctions, U.S. courts expect companies to employ a standard "custodian-based" approach with interviews of custodians. The standard approach requires the company to identify specific company employees, officers, agents, or other individuals who have access to, or administrative control over, relevant information. Once the custodians and the sources of relevant information are identified, the company typically takes action to preserve the likely sources of information identified by the custodians.

In complex litigation such as this action, litigation counsel's interviews of custodians are necessary to ascertain likely sources of relevant information. Once identified, counsel works with the company to take the steps necessary to prevent the deletion, alteration, or destruction of relevant information.

We recommend the following steps to best protect NSO against potential sanctions for failing to preserve ESI.

(1) **Suspend Automatic Deletion Protocols.** NSO must confirm that the company's systems and databases identified by the custodians as potentially relevant do not automatically delete unique ESI in any circumstances. NSO should confirm that employees' software and devices, including communications and project management software, are also not deleting unique ESI automatically. If NSO learns that any ESI is being automatically deleted, it should

---

Fla. Dec. 7, 2015); *Christensen v. Target Corp.*, 2014 WL 1224966, at *2 (D. Utah Mar. 24, 2014); *City of Lindsay v. Sociedad Quimica y Minera de Chile S.A.*, 2012 WL 2798966, at *5 (E.D. Cal. July 9, 2012); *Nursing Home Pension Fund v. Oracle Corp.*, 254 F.R.D. 559, 566 (N.D. Cal. 2008); *Sadler v. Retail Properties of Am., Inc.*, 2013 WL 12333447, at *1 (N.D. Ill. Sept. 27, 2013); *In re NTL, Inc. Sec. Litig.*, 244 F.R.D. 179, 200-01 (S.D.N.Y. 2007).

[6] *Conn. Gen. Life Ins. Co. v. New Images of Beverly Hills*, 482 F.3d 1091, 1096 (9th Cir. 2007).

immediately halt that practice and discuss with us available steps to attempt to recover deleted information.

(2) **Issue Another Legal Hold Notice.** NSO should notify all custodians that the stay does not change the custodians' obligations to preserve all hard copy records and ESI that may be related to the litigation. This notice should be written together with litigation counsel. This will prevent any possible confusion among employees about the status of the litigation and permit us to represent to the U.S. District Court that NSO sought to preserve ESI and clarify the custodians' preservation obligations if sanctions-related litigation ensues.

(3) **Conduct Custodian Interviews.** Litigation counsel should interview each likely custodian regarding any relevant information. This would allow us to assess what information must be preserved and how to best accomplish that preservation. With the assistance of litigation counsel, NSO should also develop a protocol for handling departing custodians to ensure their sources of information are properly preserved when they leave the Company. This process of interviewing custodians will help NSO (1) document its good faith efforts in identifying and preserving relevant information in compliance with U.S. law; and (2) minimize interruptions to NSO's business, including by avoiding the cost and burden of "over-preserving" information not relevant to the parties' claims and defenses.

(4) **Preserve ESI determined to be relevant to the *WhatsApp* litigation.** NSO should preserve ESI determined to be relevant to the *WhatsApp* case—as determined based on custodian interviews—by creating, as necessary, and based on the recommendations of counsel, electronic copies of those assets in a forensically sound manner.

2. *Alternative to Custodian-Based Approach: Preserve All ESI*

The alternative to interviewing custodians to limit the scope of preservation would be to preserve *all* ESI. Taking this approach, however, would be impractical, time-consuming, more expensive, and more disruptive to ordinary business operations. Accordingly, we recommend a more targeted custodian-based approach.

IV. Proposed Amendment to Israeli Seizure Order to Comply with ESI Obligations

We understand that NSO's ESI has been legally seized by the Government of Israel, although much of the information remains in NSO's physical possession. We further understand that the Government of Israel interprets the Seizure Order—which states that NSO must not change, delete, or transfer ESI to any external person or entity other than the Government of Israel—to prohibit duplication or imaging necessary for ESI preservation. And we assume that violation of the Seizure Order would carry severe penalties.

If the Seizure Order is understood to prohibit NSO from making copies of its ESI (either because the order expressly prohibits NSO from making copies or because the ESI is legally not in NSO's possession or control), we recommend NSO ask the Government of Israel to approach the Magistrate Court jointly and request that it amend the Seizure Order to permit NSO to:

(1) interview custodians and identify relevant ESI;

(2) copy relevant systems and information in NSO's possession for the purpose of complying with U.S. discovery preservation obligations; and

(3) immediately turn over ESI copies to the Government of Israel.

Preservation in this manner would allow NSO to demonstrate to the U.S. District Court it made good faith efforts to satisfy its U.S. discovery obligations. By following these steps, NSO could also mitigate future accusations, or a court finding, that it failed to take reasonable steps to preserve ESI consistent with its obligations under the Israeli Seizure Order.

If the Israeli Magistrate Court does not allow this amendment, NSO should request that the Seizure Order be amended by the Magistrate Court to make explicitly clear that NSO is not allowed to create any duplicates or copies of its ESI.

Appendix of Possible Discovery Requests[7]

Below are some examples of potentially relevant information that come directly from the discovery requests served by Facebook/WhatsApp and that would be the basis of custodian interviews.

- NSO's development, design, system architecture, testing, installation, operation, distribution, use, maintenance and/or troubleshooting relating to Pegasus, Phantom or other similar technology (RFP 1, 2, 20, 21)
- NSO's use of technology to communicate with WhatsApp, including WhatsApp servers, endpoints, computers, and computer networks (RFP 16)
- NSO's use of technology to transmit data or information from any devices containing Pegasus, Phantom or other similar technology to NSO or to NSO's customers (RFP 19)
- Pegasus Anonymizing Transmission Network (RFP 22)
- NSO's leasing of servers from third party providers in connection with the activities described in the bullets above and the locations of those servers (RFP 23)
- The use of Pegasus, Phantom or other similar technology (owned by NSO) by third parties (RFP 3, 4)
- NSO's identification of WhatsApp or Facebook application or network vulnerabilities (RFP 5, 6)
- NSO's development and testing of any technology targeting or directed at WhatsApp servers or users (RFP 7, 8, 12, 13)
- Processes, methods or technology used by NSO to monitor devices installed with Pegasus, Phantom or other similar software and exfiltrate data (RFP 9)
- Processes, methods or technology used by NSO to install Pegasus, Phantom or other similar technology on the mobile phones and devices of WhatsApp users (RFP 10, 11, 14)
- NSO's analysis, reverse engineering, disassembling, or emulating of the WhatsApp application (RFP 15)

[7] There are a few digital assets identified on the list (e.g., IPAM, DHS, DHCP (A-11-1), firewall objects (A-11-2), printer servers (A-12-1), firewall NAT+Policy Rules (A-13-12), SSO + MFA (A-13-25), vCenter (A-13-21)) that the Court may find are out of scope for preservation and discovery because they do not store relevant, unique data. Nonetheless, we would first need to interview NSO's custodians regarding these assets before advising NSO on the appropriate means of preservation, if any.

- NSO's use of WhatsApp accounts to develop, test, transmit, install, distribute, or use Pegasus, Phantom or other similar technology (RFP 17, 18)

- Data or information NSO or NSO's customers obtained through the use of Pegasus, Phantom or other similar technology (RFP 24)

- NSO's marketing, selling or promoting of Pegasus, Phantom or other similar technology (RFP 26)

- NSO's communications with Westbridge Technologies relating to WhatsApp and Facebook (RFP 28)

- NSO customers identified in Defendants' Opposition to Motion to Dismiss (RFP 25)

- NSO corporate structure and financial data (RFP 27, 29)